Migration Center

Quick Start

Issue 02

Date 2024-02-29

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Overview

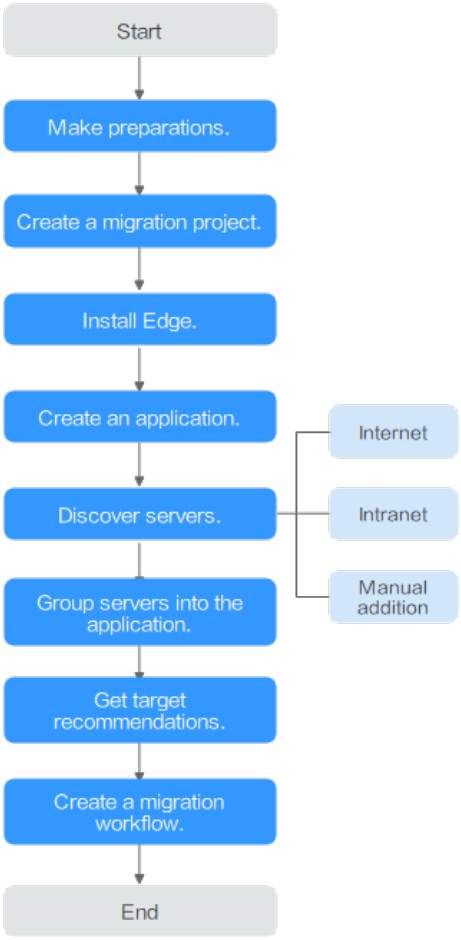
This section describes how to get started with MgC. Included are steps to introduce you to the process of using the server migration workflow of MgC.

MgC also supports cross-AZ ECS migration and storage migration. For details, see **Migrating Servers Across AZs on Huawei Cloud** and **Migrating Data from Other Clouds to Huawei Cloud**.

Flowchart

Figure 1-1 shows how to create a server migration workflow on MgC.

Figure 1-1 Process of creating a server migration workflow



2 Preparations

Before using MgC, you need to sign up for a HUAWEI ID or create an IAM user. This section describes how to sign up for a HUAWEI ID, enable Huawei Cloud, complete real-name authentication, and create an IAM user.

Signing up for a HUAWEI ID, Enabling Huawei Cloud Services, and Completing Real-Name Authentication

If you already have a HUAWEI ID, skip this part.

1. Visit **Huawei Cloud** and click **Sign Up**.
2. Sign up for a HUAWEI ID. For details, see **Registering a HUAWEI ID and Enabling Huawei Cloud Services**.
3. Complete real-name authentication.
   - If your account is an individual account, see **Individual Real-Name Authentication**.
   - If your account is an enterprise account, see **Enterprise Real-Name Authentication**.

Creating an IAM User

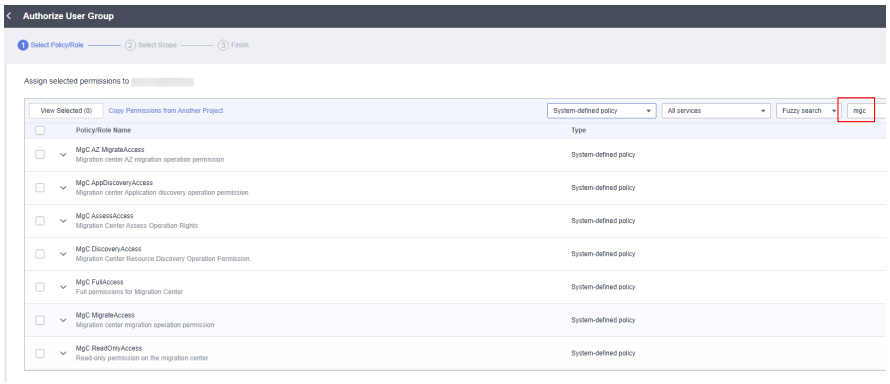
You can use your account to create IAM users to ensure the security of accounts and resources. For more information about IAM users, see **Creating an IAM User**. This section describes how to create an IAM user with permissions to access MgC. If you do not need to use any IAM users, skip this part.

1. Visit **Huawei Cloud**. Click **Console** in the upper right corner. Sign in to the console using the HUAWEI ID you signed up for.
2. Hover your cursor over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.
3. **Create a user group and assign permissions** to it.

   Create a user group. In the user group list, locate the user group you created and click **Authorize** in the **Operation** column. On the **Authorize User Group** page, search for **MgC** in the search box. Select the permissions to be assigned to the user group. For details about MgC permissions, see **Permissions Management**.

NOTE

A maximum of 20 user groups can be created.



4. **Create an IAM user and add it to the user group**.

   Create a user and add it to the user group authorized with MgC permissions in **Step 3**.

Obtaining Access Keys (AK/SK)

Access keys are identity credentials used to call APIs. The account administrator and IAM users can only use their own access keys to call APIs or perform authentication. For details about how to obtain the access keys, see **Access Keys**.

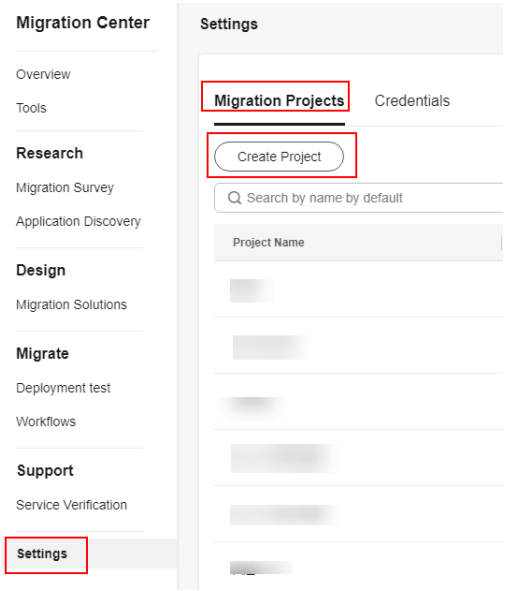
3 Creating a Migration Project

Using migration projects, you can easily isolate different migration resources. For example, you can create two different projects to isolate resources for migration from Alibaba Cloud and AWS.

Procedure

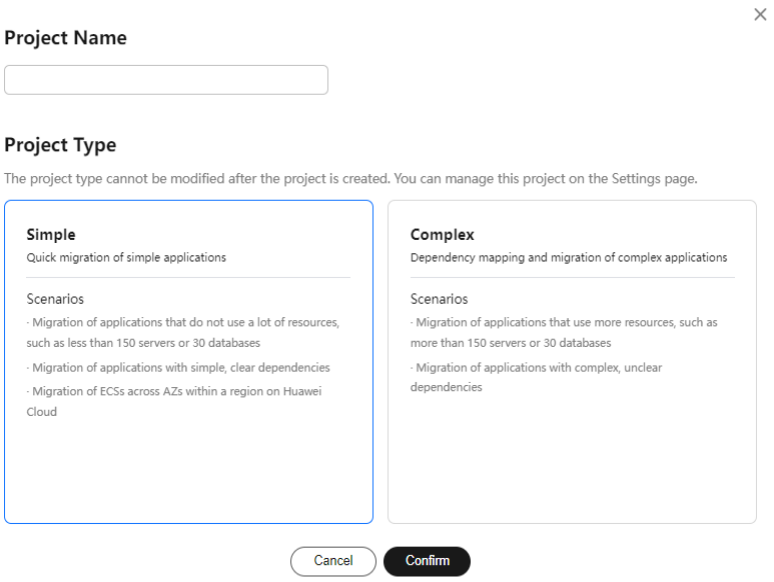
Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Settings**. On the **Migration Projects** tab page, click **Create Project**.



Step 3 In the displayed dialog box, specify a project name, select a project type as required, and click **Confirm**. The project is created, and you can view it in the migration project list.

- **Simple**: suitable for migration of a small number of applications whose dependencies are simple and clear. It is also a best choice for migration of ECSs across AZs on Huawei Cloud.
- **Complex**: suitable for migration of a large number of applications whose dependencies are complex.



----End

4 Installing Edge

4.1 Installing Edge for Windows

Preparations

- Prepare a Windows server for installing Edge in the source intranet environment. The Windows server must:
  - Be able to access the Internet and the specified **public domain names**.
  - Use PowerShell **4.0** or later.
  - Allow outbound traffic on 8883 if the server is in a security group.
- Open the required ports on source servers for communications with the server where Edge is installed.
  - Windows: port 5985
  - Linux: port 22
- Disable any antivirus and protection software on the Windows server where Edge is installed. This type of software may stop Edge from executing migration commands, resulting in migration failures.
- Enable WinRM on, if any, Windows source servers. You can run the following command and enter **y** to enable WinRM:
  ```
  winrm quickconfig
  ```
- **Sign up for a HUAWEI ID and enable Huawei Cloud services**, and obtain an AK/SK pair for the account.
- **Create a migration project** on the MgC console.

Procedure

Step 1 Log in to the **MgC** console from the Windows server you prepared.

Step 2 In the navigation pane on the left, choose **Tools**.

Step 3 In the **Windows** area, click **Download Installation Package** to download the Edge installation package to the Windows server you prepared.

Step 4 Decompress the downloaded Edge installation package, double-click the Edge installation program, and click **Next**. If the installation program cannot be

launched, try to run it in compatibility mode. For details, see **How Do I Run Edge in Compatibility Mode?**.

Step 5 On the **License Agreement** page, read the agreement carefully, select **I accept the terms of the License Agreement**, and click **Next**.

Step 6 Select drive C as the installation directory and click **Install**.

> **CAUTION**
>
> Edge can be installed only in drive C. If you select another disk for installation, Edge may fail to be started.

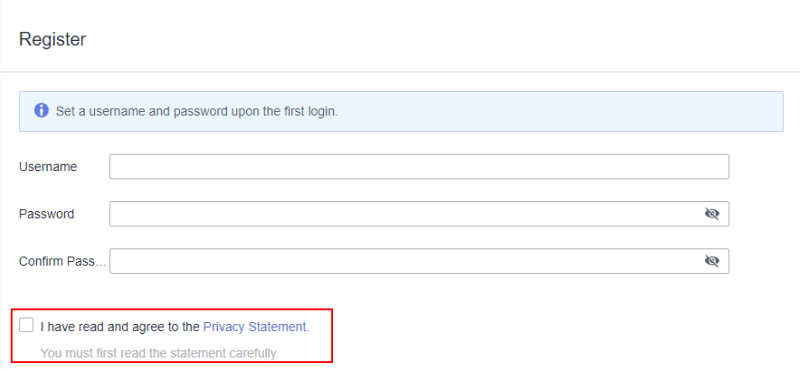
Step 7 After the installation is complete, click **Finish** to open the Edge console and go to the **User Registration** page.

----End

Registering an Account

When you log in to the Edge console for the first time, you must set a username and password. Keep the username and password secure.

Step 1 On the **Register** page, specify a username and password, confirm the password, and click **Privacy Statement**.



Step 2 Read the privacy statement carefully before selecting **I have read and agree to the Privacy Statement**, and click **Register**. Then you need to connect the Edge device to MgC. For details, see **Connecting the Edge Device to MgC**.

----End

4.2 Installing Edge for Linux

Preparations

- Prepare a Linux server for installing Edge in the source intranet environment. The Linux server must:
  - Be able to access the Internet and the specified **public domain names**.
  - Allow outbound traffic on 8883 if the server is in a security group.

  - Run CentOS 8.*X*.
  - Have at least 4 CPUs and 8 GB of memory. If you want to use big data verification, the server must have 8 CPUs and 32 GB of memory.
- Install the **rng-tools** tool on the Linux server where Edge is installed.
  - If the server runs an RPM-based Linux distribution, such as CentOS or Fedora, run the following command to install **rng-tools**:
    ```
    yum -y install rng-tools
    ```
  - If the server runs a Debian-based Linux distribution, such as Ubuntu or Debian, run the following command to install **rng-tools**:
    ```
    apt update
    apt install rng-tools -y
    ```
  - If the server runs another Linux distribution or the preceding two commands do not work, find a method of installing **rng-tools** by yourself.
- Disable any antivirus and protection software on the Linux server where Edge is installed. This type of software may stop Edge from executing migration commands, resulting in migration failures.
- Add an inbound rule to the security group of Linux server to allow TCP traffic on port 27080.
- **Sign up for a HUAWEI ID and enable Huawei Cloud services**, and obtain an AK/SK pair for the account.
- **Create a migration project** on the MgC console.

Procedure

Step 1 Log in to the **MgC** console from the Linux server you prepared.

Step 2 In the navigation pane on the left, choose **Tools**.

Step 3 In the Linux area, click **Download Installation Package** or **Copy Download Command** to download the Edge installation program to the Linux server.

Step 4 Decompress the Edge installation package.

```
tar zxvf Edge.tar.gz
```

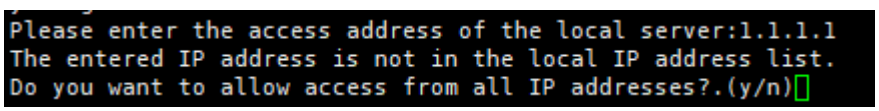
Step 5 Go to the **scripts** directory in the decompressed Edge directory.

```
cd Edge/scripts/
```

Step 6 Run the Edge installation script.

```
./install.sh
```

Step 7 Enter a private IP address of the Linux server, and the IP address will be used for accessing the Edge console. If the entered IP address is not used by the Linux server, the system prompts you whether to use any public IP address of the Linux server as the Edge access address.



Step 8 Check if the message shown in the following figure is displayed. If it is, the Edge for Linux has been installed. The port in the following figure is for reference only. Note the actual port returned.


```
There are some variables appended into /etc/profile, if you want to make these availab
le in current terminal, please run command `source /etc/profile`

Open the Edge management console by accessing https://'Available IP of local host':270
80/ from the browser.
```

Update environment variables.

```
source /etc/profile
```

Step 9 Enter **https://***IP address*:*Port number* in the address box of the browser. Replace *IP address* with the one specified in **Step 7** and *Port number* with the one returned in **Step 8**. The Edge **user registration** page is displayed.

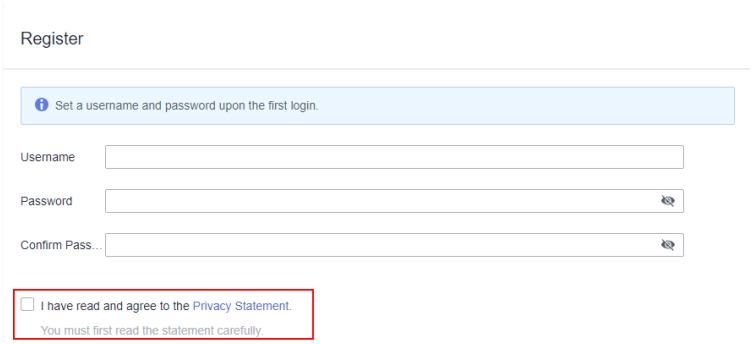
For example, if the IP address entered in step 7 is **192.168.***x.x* and the port returned in step 8 is **27080**, the Edge access address is **https://192.168.***x.x***:27080**.

----End

Registering an Account

When you log in to the Edge console for the first time, you must set a username and password. Keep the username and password secure.

Step 1 On the **Register** page, specify a username and password, confirm the password, and click **Privacy Statement**.



Step 2 Read the privacy statement carefully before selecting **I have read and agree to the Privacy Statement**, and click **Register**. Then you need to connect the Edge device to MgC. For details, see **Connecting the Edge Device to MgC**.

----End

5 Creating an Application

You can group resources with a shared business purpose as an application. The application will be used for target resource recommendation and workflow-based migration.

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Research** > **Application Discovery**. Select a **migration project** in the upper left corner of the page.

Step 3 When you access the page for the first time, click **Create Application** in the procedure.

Step 4 Enter an application name and description, select a service scenario and environment, select the region you are migrating to, and click **Create Application**. The application is created, and the page for adding resources to the application is displayed.

- If resources have been discovered, and you want to add the discovered resources to the created application, select the resources and click **Add Now**.
- If no resources have been discovered, click **Add Later**. You can add resources to the application later by referring to **Grouping Servers as Applications**.

----End

6 Discovering Servers

6.1 Discovering Servers over the Internet

This section describes how to discover servers running on clouds, such as Alibaba Cloud, Huawei Cloud, AWS Cloud, Tencent Cloud, Google Cloud, and Azure.

A simple migration project is used as an example. To learn the discovery process in a complex project, see **Discovering Resources over the Internet**.

> ⚠ CAUTION
>
> After the servers are discovered over the Internet, you need to ensure all the servers pass the pre-migration check or perform a deeper discovery for them, so that you can create a migration workflow to migrate them.

Prerequisites

- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to the Edge device.

Procedure

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Research** > **Application Discovery**. Select a **migration project** in the upper left corner of the page.

Step 3 If you are a first-time user of MgC, click **Discover Over Internet** in the **Cloud Discovery** area.

If you are not a first-time user of MgC, choose **Discover** > **Over Internet** in the **Discovery Task** card.

Step 4 Configure migration details based on **Table 6-1**.

Table 6-1 Parameters for creating an Internet-based discovery task

Area	Parameter	Description	Mandatory
Task Basics	Task Name	Enter a task name.	Yes
	Task Description	Describe the task.	No
Task Settings	Source Platform	Select the source cloud platform. Currently, Alibaba Cloud, Huawei Cloud, AWS, Tencent Cloud, Google Cloud, and Azure are supported.	Yes
	Credential	Select the credential for accessing the source cloud platform. If no credential is available, choose **Create** to create a credential by referring to **Adding a Credential**. • If the source cloud platform is Alibaba Cloud, Huawei Cloud, AWS, or Tencent Cloud, select **AK/SK** for **Authentication** and enter the AK/SK pair of your source cloud account. • If the source cloud platform is Google Cloud, select **Configuration File** for **Authentication** and upload the configuration file that contains your Google Cloud service account credentials. The file must be in JSON format and cannot exceed 4 KB. • If your source cloud platform is Azure, Select **ID/Secret** for **Authentication**. To learn how to obtain Azure credentials, see **How Do I Obtain Azure Credentials?** **NOTE** Set **Location** to **Cloud**.	Yes
	Region	Select the regions where your source services are running.	Yes

Step 5 Select **Servers** from the **Resource Type** drop-down list.

Step 6 (Optional) Group the servers to be discovered as an application.

- If an **application** is available, select the application from the **Application** drop-down list.
- If no applications are available, click **Create Application**. In the displayed dialog box, enter an application name and description, select the business scenario, environment, and region, and click **OK**.

Step 7 Click **Confirm**. An Internet-based discovery task is created, and MgC starts collecting details about source servers.

On the **Application Discovery** page, in the **Discovery Task** card, click **View** next to **Total tasks**.

Step 8 Wait until the task status changes to **Succeeded**. Then perform the following steps to check whether the source servers are ready for migration.

1. Ensure that **Edge** has been installed in the source intranet environment and has been registered with MgC.
2. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** row.
3. On the top of the server list, choose **Migration Scenario** > **Server migration**.
4. Click **Configure** in the **Migration Readiness** column.
5. Configure the parameters listed in **Table 6-2**.

Table 6-2 Migration readiness parameters

Parameter	Configuration
Type	Set this parameter based on the source server OS type.
Edge Device	Select the Edge device in the source environment.
IP Address	Select the IP address for accessing the source server. It can be a public or private IP address. If you need to use a proxy to access the server, enter the proxy IP address. After the migration readiness check is passed, the IP address will be used for subsequent migration.
Port	Enter the port on the source server opened to the Edge device. – By default, port 5985 on Windows source servers must be opened to the Edge device. The port cannot be changed. – By default, port 22 on Linux source servers must be opened to the Edge device. You can specify another port if needed.
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console and **add the server credential** to the Edge device and synchronize it to MgC.

6. Click **Confirm**. The system verifies the configuration information and starts to check whether the source server is ready for migration. If **Ready** is displayed in the **Migration Readiness** column, the source server can be migrated.

----End

6.2 Discovering Servers over an Intranet

This section describes how to discover servers in on-premises environments. Before getting started, you need to install Edge in the source environment. Then you can discover servers by network range or VMware host.

Precautions

- Only VMs in VMware vSphere 5.0 to 7.0 can be discovered.
- When the system scans VMware VMs or scans servers on specified network ranges, private IP addresses and the ID of the involved Edge device are used to identify discovered servers. If the private IP address of a discovered server, the server will be identified as a new one during the next collection, and the total number of discovered servers will increase. To avoid this, you are advised not to change private IP addresses of source servers before the migration is complete.

Prerequisites

- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to the Edge device.

Procedure

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Research** > **Application Discovery**. Select a **migration project** in the upper left corner of the page.

Step 3 If you are first-time user of MgC, click **Discover over Intranet** in the **Online On-premises Discovery** area.

If you are not a first-time user of MgC, choose **Discover** > **Over Intranet** in the **Online On-premises Discovery** pane.

Step 4 Configure migration details based on **Table 6-3**.

Table 6-3 Parameters for creating an intranet-based discovery task

Parameter	Description
Task Name	Enter a task name.
Task Description	Describe the task.
Device	Select the device where **Edge** was installed in the source intranet environment.

Step 5 Enable **Scan Network Range** or **Scan VMware VMs** to discover servers as needed.

- If **Scan Network Range** is enabled, configure parameters listed in **Table 6-4**.

  Table 6-4 Parameters for scanning a network range

Parameter	Operation
Protocol	Select the communication protocol **TCP** or **ICMP**.
Network Range	There are three supported IP address ranges: – 10.0.0.0 – 10.255.255.255 – 172.16.0.0 – 172.31.255.255 – 192.168.0.0 - 192.168.255.255
Linux	Enter the port for scanning Linux servers. This parameter is available only if you choose the TCP protocol. If you need to skip Linux servers during the scan, set this parameter to **0**.
Windows	Enter the port for scanning Windows servers. This parameter is available only if you choose the TCP protocol. If you need to skip Windows servers during the scan, set this parameter to **0**.

- If **Scan VMware VMs** is enabled, enter the IP address of a vCenter Server in the **IP Address** text box, and select the credential for accessing the vCenter Server. All VMs managed by the vCenter Server will be discovered. If the vCenter Server's credential has not been added, click **Create** to add it to MgC by referring to **Adding Resource Credentials**. When adding the credential, enter the username and password for logging in to the vCenter Server.

Step 6 Click **Confirm**. An intranet-based discovery task is created, and MgC starts discovering details about source servers.

On the **Application Discovery** page, in the **Discovery Task** card, click **View** next to **Total tasks**.

Step 7 Wait until the task status changes to **Succeeded**, and perform a deeper discovery. Servers discovered on an intranet have an Edge device associated. You only need to associated credentials with these servers before you can perform a deeper discovery.

1. On the **Application Discovery** page, click the **Resources** tab and click the number in the **Server** row.
2. Locate a server and click **Associate** in the **Credential** column.
3. Select the server credential. If the credential has not been added to MgC, go to the Edge console and **add the server credential** to the Edge device and synchronize it to MgC.
4. Click **OK**. MgC will check whether the server can be accessed using the associated credential and perform a deeper discovery. You can click

Rediscover in the **Status** column to perform a second deeper discovery if needed.

----End

6.3 Manually Adding Servers to MgC

This method is for discovering on-premises servers and cloud servers that cannot be discovered over the Internet or an intranet.

Prerequisites

- You have **installed Edge** in the source intranet environment and have connected the Edge device with MgC.
- You have **added source server credentials** to the Edge device.

Procedure

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Research** > **Application Discovery**. Select a **migration project** in the upper left corner of the page.

Step 3 If you are adding a server to MgC for the first time, choose **Add** > **Server** in the **Edge Discovery** pane.

If you have added servers to MgC before, on the **Resources** page, click **Add** on the **Servers** tab page.

Step 4 In the displayed dialog box, configure parameters listed in **Table 6-5** and click **Confirm**. MgC checks whether the server can be accessed using the specified credential and starting discovering the server details.

Table 6-5 Parameters for adding a server

Parameter	Operation
Name	Enter a server name.
Edge Device	Select the Edge device in the source environment.
Type	Select the OS type of the source server.
IP Address	Enter the IP address of the server. If the server is in the same VPC as the Edge device, you can enter the private IP address of the server. Otherwise, you have to enter its public IP address.
Port	Enter the port on the server opened to the Edge device. By default, • Port 5985 on Windows source servers must be opened to the Edge device. This port cannot be changed. • Port 22 on Linux source servers must be opened to the Edge device. You can specify another port if needed.

Parameter	Operation
Credential	Select the server credential. If the credential has not been added to MgC, go to the Edge console and **add the server credential** to the Edge device and synchronize it to MgC.

Step 5 Click the **Resources** tab on the **Application Discovery** page and click the number displayed in the **Server** row. On the **Servers** tab page, you can view the server added to MgC.

----End

7 Grouping Servers as Applications

You need to add the servers to be migrated with an application, so that you can get target resource recommendations and create a migration workflow to migrate these servers.

Procedure

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Research** > **Application Discovery**. Select a **migration project** in the upper left corner of the page.

Step 3 Click the **Resources** tab and click the number in the **Server** row.

Step 4 Select the servers to be added to the same application and choose **Resource Management** > **Manage Application Association** in the upper left corner of the page.

Step 5 Select the application from the drop-down list. If no **applications** are available, click **Create Application**. In the displayed dialog box, enter an application name and description, select the business scenario, environment, and region, and click **OK**.

Step 6 Click **OK**. You can view the application name in the **Application** column of these servers.

----End

8 Getting Target Recommendations

When assessing an application, you can get recommendations for most suitable Huawei Cloud resources based on the configuration, performance, and business scenario of the source resources added to the application, and your other requirements for, for example, cost, availability, performance, security, and compliance. You can export the assessment results as needed.

This section describes how to assess an application.

NOTE

If you have **associated source servers with target servers**, you can skip this step and create a workflow to migrate them.

Prerequisites

- You have discovered servers by referring to **Discovering Servers**.
- You have **created an application** and **associated the servers to be migrated with the application**.

Procedure

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Design** > **Migration Solutions**. Select a **migration project** in the upper left corner of the page.

On the **Migration Solutions** page, you can view the total numbers of resources, the number of resources that have target configurations, and the list of applications in the current project.

Step 3 Click **Assess** in the **Target Configuration** card.

Step 4 In the **Select Application** drop-down list, select the application for which you want to assess.

Step 5 In the **Select Resources** area, select the servers to be assessed in the application.

Step 6 Configure the assessment policy based on **Table 8-1**.

Table 8-1 Parameters for configuring an assessment policy

Parameter	Description
Target Region	Select the region where you want to purchase resources on Huawei Cloud. You are advised to select a region close to your target users for lower network latency and quick access.
Sizing Criterion	• Source specifications-based MgC recommends Huawei Cloud resources that have the same or similar specifications as source resources. • Business scenario-based MgC recommends appropriate Huawei Cloud resources based on the business scenarios of source resources and Huawei Cloud best practices. • Cross-AZ migration This policy only applies to migration of ECSs between AZs on Huawei Cloud, and MgC only assesses servers in the application. You need to select the target AZ you want to migrate to.
Preference	• Performance-first MgC recommends target resources by taking performance as the priority. • Price-first MgC recommends target resources by taking cost as the priority.
(Optional) Advanced Options	You can select ECS types, CPU types, and disk types you prefer. The configured advanced options have the highest priority during the resource assessment.

Step 7 Click **Create Assessment**. After the assessment task is complete, you can **view the assessment results** which include the recommended specifications of target resources. You can also **view server performance data**.

Step 8 (Optional) Perform the following operations:

- **Modify recommended target configurations**: You can modify recommended specifications of target servers and their disks.
- **Associate source servers with target servers**: If you already have servers that match your requirements on Huawei Cloud, you can associate them with source servers.

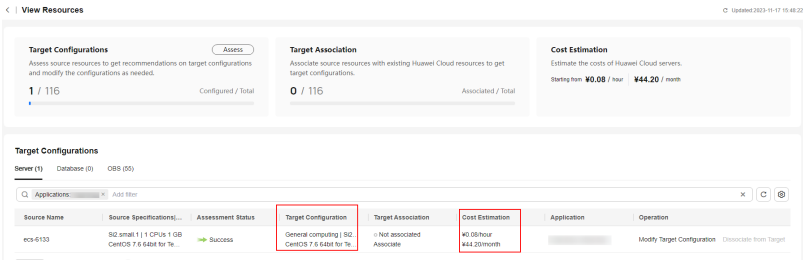
----End

Viewing the Assessment Results

In the application list on the **Migration Solutions** page, click **View Target Configurations** in the **Operation** column.

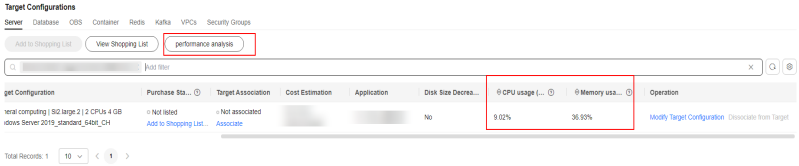
In the **Target Configurations** area, you can view the specifications of Huawei Cloud resources recommended based on the source resource specifications and

your selected preferences. It also gives you the ability to estimate what it will cost to run your services on Huawei Cloud.



Viewing Server Performance Data

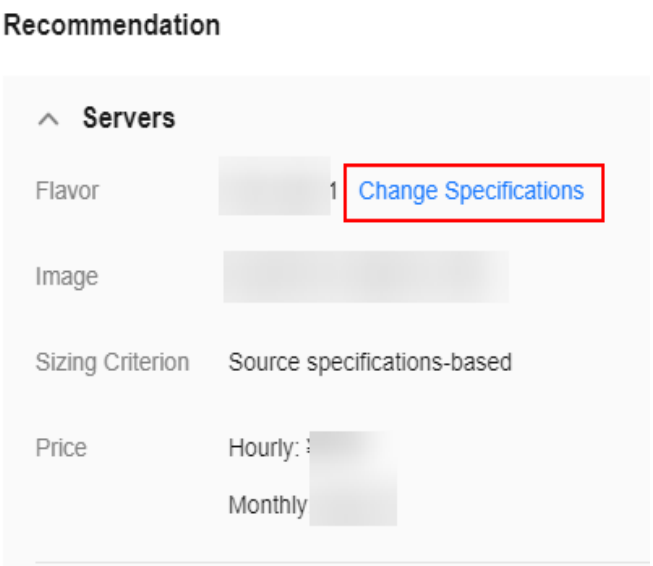
On the **Target Configurations** page, in the server list, you can view the average CPU and memory usage of each server in the last 7 or 30 days. Click **Analyze Performance** to view the performance statistics of all servers.



Modifying Recommended Target Configurations

Step 1 In the **Target Configurations** area, locate the server that you want to modify the recommended target configurations for and click **Modify Target Configuration** in the **Operation** column.

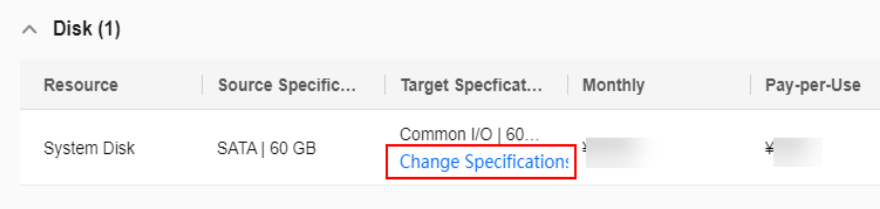
Step 2 Modify the specifications and image for the target server.



Step 3 In the disk area, locate a disk and click **Modify** in the **Target Specifications** column. You can modify the disk type and capacity. Only Linux disk sizes can be decreased. If you decrease a disk size, the system will set **Disk Size Decreased** to **Yes**. The reverse also applies.

NOTICE

- The system disk capacity ranges from 40 GB to 1,024 GB.
- The data disk capacity ranges from 10 GB to 32,768 GB.
- Only Linux disk sizes can be decreased, and decreased sizes must be larger than the used sizes of source disks.
- In the cross-AZ migration scenario, disk sizes can only be increased. Even if you decrease disk sizes here, the settings will not be applied, and the system will create target disks as large as source disks.



----End

9 Creating a Server Migration Workflow

MgC provide a server migration workflow template crafted from best practices. You can customize workflows from this template by adding tasks and steps as needed. You can run all tasks in just one click and monitor the migration progress in real time.

Prerequisites

- You have discovered servers by referring to **Discovering Servers**.
- The servers to be migrated have been **grouped as an application**.
- You have got target configurations for servers to be migrated by referring to **Getting Target Recommendations**.

Procedure

Step 1 Log in to the **MgC** console.

Step 2 In the navigation pane on the left, choose **Migrate** > **Workflows**. Select a **migration project** in the upper left corner of the page.

Step 3 Click **Create Workflow** in the upper right corner of the page.

Step 4 In the **Server Migration** card, click **Preview Steps** to view the steps predefined in the template and the detailed description of each step. If the type of a step is **Automated**, the step is automatically performed by MgC. If the type of a step is **Manual**, you need to perform the step manually. Click **Configure Workflow** in the lower right corner.

Step 5 Configure the workflow parameters based on **Table 9-1**.

Table 9-1 Parameters for configuring a server migration workflow

Area	Parameter	Operation
Workflow Details	Name	Enter a workflow name.
	Description	Describe the workflow.
Application	Application	Select the application which contains the servers to be migrated.

Area	Parameter	Operation
Migration Network	Network	If you select **Public**, ensure that all target servers have EIPs bound. These EIPs will be used for migration.
		If you select **Private**, configure Direct Connect connections, VPN connections, VPC peering connections, or subnets in the target VPC in advance to ensure that the source environment can access the target environment. • If the source environment can access the Internet over a proxy server, you need to enter the private IP address of the source proxy server and the port used by the proxy software. • If the source environment cannot access the Internet, put the SMS-Agent installation package at a location where the source servers can access directly or over a proxy. You can download the SMS-Agent installation package from the SMS console.
Target Environment	Region	Select the region you selected when you assessed the application.
	Project	Select a project in the region where the target resources are provisioned.
	VPC	• If the source IP address is 192.168.*X.X*, you are advised to create a VPC and a subnet that both belong to network range 192.168.0.0/16. • If the source IP address is 172.16.*X.X*, you are advised to create a VPC and a subnet that both belong to network range 172.16.0.0/12. • If the source IP address is 10.*X.X*, you are advised to create a VPC and a subnet that both belong to network range 10.0.0.0/8.
	Subnet	The subnet must be in the same network range as the VPC.

Area	Parameter	Operation
	Security Group	• If there are Windows source servers, the security group must be configured to allow access on ports 8899, 8900, and 22. • If there are Linux source servers, the security group must be configured to allow access on port 22. **CAUTION** – For security purposes, you are advised to only allow traffic from the source servers on these ports. – The firewall of the target servers must allow traffic to these ports.
Advanced Settings	Start Target After Migration	• If you select **No**, the target servers will be stopped after the migration is complete. • If you select **Yes**, the target servers will be started after the migration is complete.
	Set Bandwidth Limit	• If you select **No**, the migration traffic is not limited. • If you select **Yes**, you can limit the bandwidth that can be used for migration based on the source bandwidth and service requirements.
	Install rsync on Source	• If you select **No**, rsync will not be installed on the source servers. • If you select **Yes**, rsync will be automatically installed on the source servers. **CAUTION** Linux migrations depend on rsync. If rsync is not installed on a source server, the server will fail to be migrated.
	Enterprise Project	Select the enterprise project you want to migrate to. The enterprise project **default** is selected by default.

Step 6 Click **Next: Confirm**.

Step 7 Confirm the workflow settings, and click **Confirm**. The **Run Workflow** dialog box is displayed, which indicates that the workflow has been created.

- If you want to start the migration immediately, click **Confirm** to run the workflow.
- If you want to **add stages** and **add steps** to the workflow, click **Cancel**. The workflow enters a **Waiting** state, and the migration is not started. To start the migration, click **Run** in the **Operation** column.

Step 8 On the migration workflow details page, view the workflow settings and the migration progress.

- Move the cursor to the migration progress bar. In the box that is displayed, view more migration details.
- When the migration progress bar reaches a step that requires manual confirmation, move the cursor to the progress bar and click **Confirm** next to the step status in the displayed window, so that the subsequent migration steps can be executed.
- When the workflow reaches the **ResizeDiskPartition**, the system identifies whether disk capacity reduction has been performed on the target server.
  - If yes, go to **SMS console** and resize disks and partitions for the target server. For details, see the **Partition Resizing** parameter in **Configuring a Target Server**. After the adjustment is complete, go back to the MgC console and click **Confirm** next to the step status so that the workflow can continue.
  - If no, skip this step.
- The **StartSynchronization** step is repeated before you verify your services.

----End

Adding a Stage

Step 1 On the migration workflow details page, move the cursor to the migration stage before or after which you want to add a stage. In the displayed window, choose **Add Stage Before** or **Add Stage After**.

Step 2 Enter a stage name and description, click **Add Step**, select a step type, enter a step name and description, and click **Confirm**. Multiple steps can be added.

Step 3 Click **Confirm**.

NOTICE

Manually added stages can be modified or deleted, but pre-defined stages cannot.

----End

Adding a Step

Step 1 On the migration workflow details page, move the cursor to the step before or after which you want to add a step. In the displayed window, choose **Add Step Before** or **Add Step After**.

Step 2 Select a step type based on **Table 9-2**, enter a step name and description, and click **Confirm**.

Table 9-2 Step types

Type	Description
Checkpoint	You need to manually confirm this type of steps, so that the workflows can continue.

Step 3 Go back to the migration stage and view the added step.

NOTICE

Manually added steps can be modified or deleted, but pre-defined steps cannot.

----End

10 Change History

Released On	What's New
2024-02-29	This issue is the second official release. Add the description of migration pre-check to **Discovering Servers over the Internet**.
2023-10-30	This issue is the first official release.

